UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

IN RE: PRACTICEFIRST DATA BREACH LITIGATION

This Document Relates To: All Actions

Master File No. 1:21-cv-00790- JLS

DEFENDANTS' MEMORANDUM OF LAW
IN SUPPORT OF THEIR MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), Defendants Professional Business Systems, d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp. (collectively, "Defendants") submit this memorandum of law in support of their motion to dismiss Plaintiffs' Consolidated Class Action Complaint, ECF No. 22 ("Complaint" or "Compl.") with prejudice.

INTRODUCTION

This case stems from an alleged December 2020 incident during which cybercriminals gained unauthorized access to Defendants' systems through a ransomware attack and encrypted certain data. Putative class actions like the one filed by Plaintiffs following a cybersecurity incident have proliferated over the last decade. However, this data breach class action is distinct from the majority of others in one material aspect: Defendants have no direct relationship with the Plaintiffs.

The attenuation in the parties' relationship is fatal to Plaintiffs' claims. Plaintiffs' negligence and injunctive relief claims (Counts I and III) fail because Defendants do not owe Plaintiffs (third parties with whom it has no direct relationship) a duty of care to protect them against the criminal acts of malicious third parties. Plaintiffs resort to federal statutes to manufacture a duty of care, but none of those statutes contain a private right of action. Plaintiffs also cannot use tort law to create a right that Congress chose not to enact. Moreover, foreseeability alone is not sufficient to create a duty of care. In short, this Court should reject Plaintiffs' effort to manipulate tort law into a mechanism to enforce Defendants' contracts with its clients.

Recognizing this defect, Plaintiffs attempt to manufacture a breach of contract claim (Count II) based on contracts the Defendants had with the various healthcare facilities at which Plaintiffs obtained medical services. Plaintiffs claim that they can sue under those contracts

because "one of the subjects" of Defendants' contracts is the maintenance of patient data. However, it is black letter law in New York that non-parties to a contract do not have standing to sue under contract absent an express contract provision. Plaintiffs do not plausibly allege the existence of any such contract language.

Finally, Plaintiffs fail to allege any cognizable damages. None of the Plaintiffs allege that they have actually experienced any identity theft as a result of the subject ransomware attack. Rather, Plaintiffs base their damages claim primarily on a potential risk of future identity theft. Yet, Plaintiffs' own allegations concede that the risk of such identity theft is neither likely nor imminent, rendering their damages claims too speculative and remote to constitute any legally recognizable relief. For all of these reasons, this Court should dismiss Plaintiffs' entire complaint with prejudice.

PLAINTIFFS' ALLEGATIONS

Plaintiffs allege that Defendants are a "medical management solutions company" that "provides administrative and back-office services to medical professionals," including services such as billing, credentialing, coding, bookkeeping, and tax preparation. (Compl. ¶¶ 2-3). Plaintiffs allege that Defendants entered into contracts to provide practice management services to medical providers, including medical providers used by the Plaintiffs. (Compl. ¶¶ 2-3, 127).

Plaintiffs allege that cybercriminals executed a ransomware attack that encrypted information on Defendants' systems in December of 2020. (Compl. ¶ 4). Defendants subsequently notified Plaintiffs and other patients and employees of Defendants' clients that their personally identifiable information ("PII") and protected healthcare information ("PHI") may have been accessed by the criminal actor. (Compl. *e.g.,* ¶ 6). This notification was necessitated by state data breach reporting law.

Plaintiffs allege that "although the information accessed and stolen varies by individual, the categories of patient and employee data obtained by the hackers included: names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnoses, laboratory and treatment information, patient identification numbers, employee username and passwords, employee username with security questions and answers, and bank account and/or credit card/debit card information." (Compl. ¶ 5). None of the Plaintiffs articulate which particular form of their data was accessed, if any. *See generally* Compl. Plaintiffs admit that Defendants notified them that the ransomware actor confirmed that it had permanently deleted any exfiltrated data after Defendants responded to the subject incident. (Compl. ¶ 21).

Plaintiffs assert three causes of action stemming from the incident: (1) breach of contract as intended-third party beneficiaries (2) negligence; and (3) declaratory and injunctive relief. *See generally* Compl. Plaintiffs claim that they suffered the following damages from the incident: (1) the alleged risk of future identity theft (Compl. ¶ 122(g); (2) time and expenses associated with their attempts to protect against that alleged risk (Compl. ¶ 122(c)-(f), (h)); (3) loss of the benefit of their bargain with Defendants (Compl. ¶ 122(a)); and (4) diminished value of their PII/PHI. (Compl. ¶ 84). None of the Plaintiffs allege that they have actually experienced any identity theft as a result of the subject incident. *See generally* Compl.

STANDARD OF REVIEW

To establish Article III standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief. *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2203 (2021). "A plaintiff must demonstrate standing separately for each form of relief sought." *Id.* at 2210. When a Rule 12(b)(1) motion is facial, *i.e.*, based solely on the allegations of the complaint, "the task of the district court is to

determine whether the complaint alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue." *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2nd Cir. 2016).

To survive a motion to dismiss pursuant to Rule 12(b)(6), a complaint must provide "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The Court must accept as true all factual allegations in the complaint and draw all reasonable inferences in the plaintiff's favor. *See E.E.O.C. v. Port Auth. of N.Y. & N.J.*, 768 F.3d 247, 253 (2nd Cir. 2014). "At the same time, however, a plaintiff's obligation requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Zembiec v. County of Monroe*, 766 F.Supp.2d 484, 491–92 (W.D.N.Y. 2011), *quoting Bell Atl. Corp.*, 550 US. At 555. "Factual allegations must be enough to raise a right to relief above the speculative level." *Id.*

ARGUMENT

As explained in Section I, this Court should dismiss Plaintiffs' contract and negligence claims to the extent they seek monetary damages because Plaintiffs fail to plausibly allege the existence of an injury-in-fact sufficient to satisfy Article III of the U.S. Constitution. Similarly, as explained in Section IV, this Court should dismiss Plaintiffs' contract and negligence claims because Plaintiffs' fail to plausibly allege the existence of any category of damages that is cognizable under New York law.

As explained in Section II, this Court should dismiss Plaintiffs' breach of contract claim (Count II) under Rule 12(b)(6) because Plaintiffs have failed to allege the existence of a contract with express language clearly granting Plaintiffs standing to sue as intended third-party beneficiaries.

As explained in Section III, this Court should dismiss Plaintiffs' negligence claim (Count I) under Rule 12(b)(6) because Defendants to not owe a duty of care to Plaintiffs (third parties with whom Defendants have no direct relationship) to protect against criminal acts of other third-parties). Plaintiffs' negligence claim also fails because Plaintiffs fail to allege facts showing that: (a) Defendants were on notice of any defects in their security measures, and (b) that the alleged criminal activity was foreseeable.

I. In light of *TransUnion*, Plaintiffs have failed to establish standing for monetary damages, because Plaintiffs concede that their risk of identity theft is not certainly impending, and Plaintiffs cannot establish any concrete injury based solely on such speculative risk.

The Supreme Court in *TransUnion LLC v. Ramierz,* 141 S.Ct. 2190, 2210 (2021), recently explained that "[a] plaintiff must demonstrate standing separately for each form of relief sought" to meet Article III's injury-in-fact standing requirement. Accordingly, "a plaintiff's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages." *Id.* Regarding injunctive relief, "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id., citing Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 410 (2013) (to confer standing, the risk of future injury must be "certainly impending"). However, "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm." *Id.* at 2210-2211.

Here, none of the Plaintiffs allege that they have actually experienced any identity theft. Rather, Plaintiffs premise their damages allegations on the risk of identity theft occurring in the future. (Compl. ¶ 7). Further, Plaintiffs' own allegations concede that the risk of any identity theft occurring is neither probable nor imminent. Specifically, regarding probability, Plaintiffs allege that "according to experts, one out of four data breach notification recipients become a

victim of identity fraud." (Compl. ¶ 63). Accepting for purposes of this motion only Plaintiffs' cited metric, each of their chances of experiencing identify theft is approximately 25%, which is neither probable nor likely.[1] (Compl. ¶ 63); *See Khan v. Children's Nat'l Health System*, 188 F.Supp.3d 524, 533 (D. Md. 2016) (statistics that 19 percent of data breach victims become victims of identity theft, "which are cited in numerous other cases, do not by themselves establish that there is certainly impending harm"). Regarding timing, Plaintiffs further allege that "data thieves may wait years before attempting to use the stolen PII/PHI" and that any identify theft may not occur "for years or even decades to come." (Compl. ¶ 54).

By Plaintiffs' own allegations then, their risk of future injury is neither "certain" nor "impending." *Clapper*, 568 U.S. at 410 (rejecting use of "objectively reasonable likelihood" standard and explaining that the risk of future injury must be "certainly impending"). Indeed, it has been nearly one full year since the subject incident in December 2020 and none of the Plaintiffs have alleged any actual instances of identity theft, despite the recent opportunity to consolidate and amend their complaint. *See Fero v. Excellus Health Plan, Inc.*, 236 F.Supp.3d 735, 753 (W.D.N.Y. 2017) (plaintiffs' failure to allege any actual misuse of their data in three years since breach "undercuts their assertion that the asserted harm of future identity theft is certainly impending"); *Whalen v. Michael Stores, Inc.*, 153 F.Supp.3d. 577, 583 (E.D.N.Y. 2015) (risk of identity theft was not certainly impending when plaintiff alleged that it might not occur for years, and two years had transpired since the data breach without any fraudulent activity); *In*

---

[1] Contrary to Plaintiffs' cited metric, the Government Accountability Office (GAO) report cited by Plaintiffs in their Complaint found that "most breaches have not resulted in detected incidents of identity theft." (Compl. ¶ 71, n. 27) *citing* GAO, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited (June 2007), https://www.gao.gov/assets/gao-07-737.pdf. Specifically, the GAO found that for 24 of the largest breaches between 2000 and 2005, only 3 resulted in identity theft, for a rate of ***only 12.5%***, which only further demonstrates that any identity theft is not certainly impending.

re Zappos.com, Inc., 108 F.Supp.3d 949, 958 (D. Nev. 2015) ("The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial").

Plaintiffs' concession that their risk of future injury is neither likely nor imminent means that Plaintiffs cannot establish that they have any standing to pursue damages based solely on "exposure to the risk of future harm itself." *TransUnion*, 141 S.Ct. at 2210-2211. The same standard of review applies to Plaintiffs' claims that each took measures to mitigate against this speculative future risk. Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416. Further, as the Second Circuit has acknowledged, "where plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 303 (2nd Cir. 2021).[2] Plaintiffs' present injury claims based on their anxiety and mitigation measures taken in response to an admittedly speculative risk of future harm are insufficient to confer Article III standing for compensatory damages. Accordingly, Plaintiffs' claims for damages must be dismissed for lack of standing.

---

[2] *McMorris* was decided prior to the Supreme Court's declaration in *TransUnion* that "in a suit for damages [as opposed to injunctive relief], the mere risk of future harm, standing alone, cannot qualify as a concrete harm." 141 S.Ct. at 2210-2211. While *McMorris* held that the plaintiff in that case failed to establish standing, *McMorris* explained that the risk of future identity theft might be sufficient to confer standing in a data breach lawsuit depending on an analysis of three stated factors. 995 F.3d 295. However, *McMorris* did not distinguish between claims for damages and claims for injunctive relief. 995 F.3d 295. With respect to claims for damages, *TransUnion* effectively abrogates *McMorris*' three-factor test, and that test is not applicable to Plaintiffs' claims for damages in light of *TransUnion*.

II. This Court should dismiss Plaintiffs' breach of contract claims because Plaintiffs cannot establish that that they are intended third-party beneficiaries of Defendants' contracts with medical providers.[3]

Plaintiffs allege that they are intended third-party beneficiaries of Defendants' contracts with Plaintiffs' medical providers merely because the Plaintiffs' PII/PHI "is one of the subjects of [Defendants'] contracts." (Compl. ¶ 128). Plaintiffs' claim fails because they fail to allege any facts demonstrating the existence of a clear contractual language granting Plaintiffs a contractual right to sue under those contracts.

"Parties asserting third-party beneficiary rights under a contract must establish (1) the existence of a valid and binding contract between other parties, (2) that the contract was intended for their benefit and (3) that the benefit to them is sufficiently immediate, rather than incidental, to indicate the assumption by the contracting parties of a duty to compensate them if the benefit is lost." *Mendel v Henry Phipps Plaza W.*, 811 N.Y.S.2d 294 (NY Ct. App. 2006). "A third party is an intended beneficiary where either (1) 'no one other than the third party can recover if the promisor breaches the contract' or (2) 'the language of the contract otherwise clearly evidences an intent to permit enforcement by the third party.'" *Akcess Pac. Grp. LLC, v. Winstar Comm's, Inc.*, 67 F.Supp.2d 394, 399 (S.D.N.Y. 1999), *quoting Fourth Ocean Putnam Corp. v. Interstate Wrecking Co., Inc.*, 66 N.Y.2d 38, 45 (NY Ct. App. 1985). "The parties' intent to benefit the third party must be apparent from the face of the contract." *LaSalle Nat. Bank v Ernst & Young LLP*, 285 A.D.2d 101, 108 (1st Dept. 2001). "Absent clear contractual language evincing such intent, New York courts have demonstrated a reluctance to interpret circumstances to construe such an intent." *Id.* at 108-109.

---

[3] Plaintiffs have not attached or pled the terms of any applicable contract. For the purpose of this motion, Defendants assume New York law applies to Plaintiffs' contract claims. However, Defendants do not concede that New York law would apply to every contract applicable to the putative class.

Here, Plaintiffs' allegations show that they can be no more than incidental beneficiaries of the Defendants' contracts with the Plaintiffs' medical providers. Plaintiffs allege that Defendants are a "medical management solutions company" that "provides administrative and back-office services to medical professionals," including services such as billing, credentialing, coding, bookkeeping, and tax preparation. (Compl. ¶¶ 2-3). Of course, the intended beneficiary of these medical practice management services are the medical providers themselves. Plaintiffs claim that they are beneficiaries of Defendants' contracts, however, because their data "is one of the subjects of the contracts." (Compl. ¶ 128). To the extent that Defendants' services involve the processing of Plaintiffs' data on behalf of Defendants' clients, those services primarily, if not exclusively, benefit Defendants' medical provider clients, and not the Plaintiffs.

Plaintiffs have not alleged any facts that could establish that they are the *only* ones who can recover if Defendants breach their contracts with the medical providers, a necessary element of demonstrating one's status as a third-party beneficiary. *Akcess Pac. Grp.,* 67 F.Supp.2d at 399 ("A third party is an intended beneficiary where […] no one other than the third party can recover if the promisor breaches the contract"). Of course, the medical providers can seek to enforce the provisions of their own contracts. *See Id.* (finding no third-party beneficiary status when the actual party to the contract "obviously had the power to enforce its terms").

Further, Plaintiffs have not alleged any facts that could establish that Defendants and their clients clearly intended to grant Plaintiffs any third-party enforcement rights with respect to their contract. As an initial point, Plaintiffs have not cited any language of the contracts at all, let alone "clear contractual language evincing such intent" to confer third-party beneficiary status.

LaSalle Nat. Bank, 285 A.D.2d at 108. This alone is fatal to their third-party beneficiary claim under New York law.[4]

More relevant to the instant subject matter, in a data breach lawsuit, this Court has found that plaintiffs were not intended third-party beneficiaries of their health insurer's agreement with the federal government that included patient data security provisions for data processing, even when that agreement explicitly created a procedure for patients to submit billing and benefits disputes, when that agreement did not explicitly create any similar right for patients to enforce the data security provisions. *Fero*, 236 F.Supp.3d at 769 (W.D.N.Y. 2017) (Hon. J. Wolford) (dismissing third party beneficiary claim and holding that "silence cannot be interpreted to manifest a clear intent to permit enforcement").

Here, Plaintiffs have not alleged any contractual language evidencing a clear intent to grant the Plaintiffs third-party enforcement rights with respect to any provisions in Defendants' contracts. *See James v. Countrywide Fin. Corp.*, 849 F.Supp.2d 296 (E.D.N.Y. 2012) (dismissing breach of contract claim for failure to sufficiently allege the existence of an agreement, explaining that while a plaintiff "need not attach a copy of the contract to the complaint …, the complaint must at least set forth the terms of the agreement upon which liability is predicated by express reference"). Rather, Plaintiffs have alleged only that they are incidental beneficiaries of Defendants' contracts, which is not enough to establish that the

---

[4] As an example of the high bar the Plaintiffs need to surmount for third party beneficiary status in New York, in *Ralston Purina Co. v Arthur G. McKee & Co*., the court found that the owner of an industrial facility was an intended third-party beneficiary of a roofing subcontractor's agreement with the general contractor to install a roof for the facility, when the subcontractor's agreement expressly extended the subcontractor's warranties to the owner, the subcontractor agreed to indemnify the owner for any damages arising out of the subcontractor's work on the project, *and* the subcontractor agreed to be bound by the provisions in the general contractor's own agreement with the owner. 158 A.D.2d 969, 970 (4th Dept. 1990). Plaintiffs do not plead the existence of similar provisions in any of Defendants' agreements with its various clients.

contracting parties intended to grant Plaintiffs any third-party enforcement rights. Accordingly, this Court should dismiss Plaintiffs' breach of contract claims.

III. This Court should dismiss Plaintiffs' negligence claim because Defendants did not owe Plaintiffs any duty to protect them from the criminal acts of third parties, and Plaintiffs have not plausibly alleged notice or reasonable foreseeability of any such criminal acts.

Plaintiffs allege that Defendants owed Plaintiffs a duty of care based on its contracts with the medical providers, and certain standards of the Health Insurance Portability and Accountability Act ("HIPAA") and the Federal Trade Commission Act ("FTCA"). (Compl. ¶¶ 110-113). Plaintiffs contend that Defendants breached these duties "because of their unsecure and inadequate data security practices and procedures." (Compl. ¶ 4). Beyond these conclusory allegations, Plaintiffs do not allege any further detail regarding the cause of the subject ransomware attack or relating the allegedly inadequate data security practices to the attack.

First, Plaintiffs' negligence claim fails because Defendants do not owe a duty of care to Plaintiffs (third parties with whom Defendants have no direct relationship) to protect against criminal acts of third parties. Next, Plaintiffs' negligence claim also fails because Plaintiffs fail to allege facts showing that: (a) Defendants were on notice of defects in their security measures, and (b) that the alleged harm to Plaintiffs was foreseeable.

A. This Court should dismiss Plaintiffs' negligence claims because Defendants did not have any relationship with the Plaintiffs that gives rise to a duty to protect Plaintiffs from the criminal acts of third parties.

Defendants do not have any relationship with the Plaintiffs that could give rise a duty to protect the Plaintiffs from the criminal acts of third-party ransomware attackers as a matter of law. "A defendant generally has no duty to control the conduct of third persons so as to prevent them from harming others, even where as a practical matter defendant can exercise such control." *Hamilton v Beretta U.S.A. Corp.*, 96 N.Y.2d 222, 233 (NY Ct. App. 2001). "Generally, such a duty may arise only where there is a relationship either between defendant and a third-

person tortfeasor that encompasses defendant's actual control of the third person's actions, or between defendant and plaintiff that requires defendant to protect plaintiff from the conduct of others." *In re New York City Asbestos Litigation*, 806 N.Y.S.2d 146, 149–50 (NY Ct. App. 2005). "Examples of these [special] relationships include master and servant, parent and child, and common carriers and their passengers." *Id.* "Without a duty running directly to the injured person there can be no liability in damages, however careless the conduct or foreseeable the harm." *Hamilton*, 96 N.Y.2d at 232. ***"Foreseeability, alone, does not define duty—it merely determines the scope of the duty once it is determined to exist.***" *Id. (emphasis added).*

B. Contractual obligations do not give rise to a tort duty, and Defendants' contracts do not meet any of the three limited exceptions to that rule.

Plaintiffs admit that Defendants have no direct relationship with the Plaintiffs. Rather, Defendants have contractual relationships with various medical providers, and the Plaintiffs allege that they were patients of some of those medical providers. The mere fact that Defendants had contracts with the Plaintiffs' medical providers does not give rise to a duty owed to the Plaintiffs. "A contractual obligation, standing alone, will generally not give rise to tort liability in favor of a third party" *Espinal v. Melville Snow Contrs.*, 98 N.Y.2d 136, 138 (2002) (finding that snow removal contractor did not owe any duty of care to customers of contractor's client), *citing Eaves Brooks Costume Co. v Y.B.H. Realty Corp.*, 76 N.Y.2d 220, 226 (NY Ct. App. 1990) (affirming dismissal of negligence claims brought by warehouse tenant against the warehouse owner's contractor, finding that the contractor did not owe any duty to the tenant to protect the tenant's personal property from damage, and tenant could pursue breach of contract claim against the owner). The New York Court of Appeals recently reiterated Chief Judge Cardozo's admonition that "imposing liability under such circumstances could render contracting parties liable in tort to an indefinite number of potential beneficiaries" and the New York courts have "rejected the concept of open-ended tort liability." *Id.*, *citing H.R. Moch Co., v. Rensselaer*

Water Co., 247 N.Y. 160, 168 (1928) (finding that water utility company that had contract with city did not owe any duty of care to property owner who alleged that his property burned because the utility failed to supply adequate water pressure to city fire hydrants).

Rather, the New York Court of Appeals has recognized only three exceptions to the general rule that a contractual undertaking does not give rise to a duty of care to third parties. The three established exceptions are where: (1) a contracting party "launches a force or instrument of harm;" (2) "where the plaintiff detrimentally relies on the continued performance of the contracting party's duties;" and (3) "where the contracting party has entirely displaced the other party's duty to maintain the premises safely"). *See Espinal*, 98 N.Y.2d at 140. None of these exceptions apply here.

1. The first exception does not apply because Defendants did not "launch a force or instrument of harm."

Plaintiffs have not alleged facts showing that that Defendants "launched a force or instrument of harm." *Id.* In *Landon v. Kroll Laboratory Specialists, Inc.*, 22 N.Y.3d 1 (2013), the New York Court of Appeals elaborated on this exception when it found that a drug testing laboratory that had a contract with a county probation department owed a duty of care to drug test subjects. In that case, a probationer alleged that the laboratory issued a false positive drug test that caused the county to find that the probationer violated the terms of his probation. *Id*. at 6. The Court of Appeals explained that the laboratory "launched a force or instrument of harm" because it was the probationer's "own biological specimen that was the **sole** subject of the testing" and the probationer was "**directly harmed**" by the false positive test that threatened his right to freedom. *Id.* at 6 (emphasis added). The facts in *Landon* are entirely distinguishable from the present case. Defendants' generalized practice management services here are entirely distinguishable from the drug testing services in *Landon* that were specific to the plaintiff's physical specimen and resulted in the direct misrepresentation of the plaintiff's probation

compliance. The alleged incident here is a third-party criminal attack on Defendants' systems, not a service for or false representation regarding any of the Plaintiffs.

2. The second exception is not applicable because Plaintiffs cannot plausibly allege detrimental reliance.

The Plaintiffs do not allege that they were aware of Defendants' contracts with their medical providers, let alone plausibly allege that they detrimentally relied upon Defendants' performance under its contracts. More importantly, Plaintiffs cannot show plausible show detrimental reliance because the primary purpose of Defendants' contracts with its business clients was to provide medical practice management services (like billing and accounts receivables). Access to patient data (billing codes, names, *etc.*) was merely incidental to the primary purpose of servicing those business contracts for clients.

For that reason, this case is distinguishable from the one recent out-of-circuit data breach case to have found a duty of care based on a contractual undertaking. *See In re Blackbaud, Inc., Customer Data Breach Litigation,* 2021 WL 4866393, at *8 (D.S.C., Oct. 19, 2021). In that case, the district court, applying South Carolina law, declined to dismiss a negligence claim after finding that this exception could apply because the defendant was a third-party data services provider and the "primary purpose" of its contracts "was to maintain and secure" plaintiff's data. The facts as pled by Plaintiffs here demonstrate the incidental, and not primary, purpose of data processing to Defendants' medical practice management services.

3. The third exception does not apply because Defendants did not entirely displace the services of Plaintiffs' medical providers.

Finally, Plaintiffs have not plausibly alleged that Defendants' services entirely displaced the medical providers' own responsibility for Plaintiffs' PII/PHI. Rather, Plaintiffs admit that their relationship was with their medical providers, who collected their information in the first instance. Compl. ¶¶ 103. 112. Therefore, the third exception is also inapplicable. *See Palka v.*

Servicemaster Mgm't Services, Corp., 83 N.Y.2d 579 (1994) (finding that property management company owed duty of care to hospital employees, where management company had complete management responsibilities for hospital and company interacted directly with hospital employees to address maintenance issues). Plaintiffs' negligence claim should be dismissed.

C. Federal law also does not create a tort duty.

Aside from Defendants' contracts, the mere fact that HIPAA or the FTCA establish some standards regarding data security does not work to create a tort duty of care absent a special relationship. "Time and again we have required … that the damaged plaintiff be able to point the finger of responsibility at a defendant owing, not a general duty to society, but a specific duty to him." *Lauer v. City of New York*, 95 N.Y.2d 95, 100 (2000). Further, neither HIPAA nor the FTCA contain a private right of action, and multiple courts have rejected plaintiffs' attempts to manipulate tort law to manufacture a private right of action that Congress chose not to enact. *See Alfred Dunhill, Ltd., v. Interstate Cigar Co.,* 499 F.2d 232, 237 (2nd Cir. 1974) ("Nowhere does the [FTCA] bestow upon either competitors or consumers standing to enforce its provisions"); *In re GE/CBPS Data Breach Litigation*, 2021 WL 3406374, at *10 (S.D.N.Y. 2021) (collecting cases dismissing negligence *per se* claims in data breach litigation based on alleged violations of the FTCA); *Romanello v. Intesa Sanpaolo S.p.A.*, 949 N.Y.S.2d 345, 352 (1st Dept. 2012) (dismissing privacy claim based on alleged HIPAA violation because HIPAA does not create a private right of action).

Consistent with this analysis, the Southern District of New York dismissed a negligence claim against a bank in data breach litigation, finding that the bank did not owe any duty to plaintiffs who were not direct customers of the bank, and instead were customers of some of the bank's institutional clients, such as Walt Disney. *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307 (S.D.N.Y. June 25, 2010); *See also Willingham v. Global Payments,*

Inc., 2013 WL 440702, at *18 (N.D. Ga., Feb. 5, 2013) ("no duty of care exists in the data breach context where, as here, there is no direct relationship between the plaintiff and the defendant"). Further, multiple courts have dismissed negligence claims in data breach litigation where the state legislature at issue had enacted data security and/or data breach notification laws but declined to authorize a private right of action. *See In re Anthem, Inc. Data Breach Litigation*, 162 F.Supp.3d 953 (N.D. Cal. 2016) (dismissing negligence claim where state law at issue authorized only attorney general to prosecute violations of state data security and data breach notification laws); *Worix v. MedAssets, Inc.*, 869 F.Supp.2d 893, 897-898 (N.D. Ill. 2012) (dismissing negligence claim, refusing to recognize a "new common law duty to safeguard information," and refusing to create "a new legal duty beyond legislative requirements already in place"); *Amburgy v. Express Scripts, Inc.*, 671 F.Supp.2d 1046 (E.D. Mo. 2009) (same).

Same as with the states in these cases, the New York legislature enacted data security and data breach notification laws prior to the subject incident, but the legislature chose not to authorize a private right of action for any violations of those laws. *See* G.B.L. §§ 899-AA, 899-BB. Thus, following that same analysis, this Court should dismiss Plaintiffs' negligence claims because Defendants do not have any relationship with Plaintiffs, let alone a legally special relationship, that could give rise to a duty to protect the Plaintiffs from the criminal acts of third parties.[5]

---

[5] Based on the lack of any direct relationship between Defendants and Plaintiffs, the subject litigation is distinguishable from data breach cases where a duty of care was found, because the defendants in those cases had a direct relationship with the Plaintiffs. *See In re GE/CBPS*, 2021 WL 3406374 (S.D.N.Y. 2021) (employer-employee relationship); *Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739 (S.D.N.Y. 2017) (same); *Wallace v. Health Quest Systems, Inc.*, 2021 WL 1109727 (S.D.N.Y. Mar. 23, 2021) (medical provider-patient relationship); *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F.Supp.3d 1295, 1309 (N.D. Ga. 2019) (consumer credit reporting agency that had direct relationship to plaintiffs because it "sells [credit reports] directly to consumers"); *In re Experian Data Breach Litigation*, 2016 WL 7973595 (C.D. Cal., 2016) (same as *Equifax*).

D. This Court should also dismiss Plaintiffs' negligence claims because Plaintiffs failed to allege any facts that could plausibly establish that Defendants had notice of any defects in its security measures.

As explained in Section III (A-D), Plaintiffs' complaint fails to establish that Defendants owed them any duty of care. Even assuming *arguendo* that a duty existed, Plaintiffs' negligence claim also fails because Plaintiffs' do not allege any facts that could plausibly establish that Defendants had defective security measures *and* had notice of such defect which could constitute the ***breach*** of any duty, assuming ***arguendo*** that one was owed. New York courts have recognized that in instances where a duty of care to protect against the criminal acts of third parties may arise, such as in the context of landowners and landlords relative to their guests and tenants, the plaintiff must also show the defendant had notice of a safety or security defect.

In that context, for example, a landowner is not liable for the criminal acts of third parties that were enabled by a safety defect on the premises *unless* the landowner had prior notice of the security defect. *See Batista v. City of New York*, 970 N.Y.S.2d 197 (1st Dept. 2013) (landowner not liable for assault committed on premises when landowner had no notice of any defects in the building door locks). Notice can be either actual or constructive, but constructive notice will not arise unless the defect was "apparent" and "existed for a sufficient period of time" that the landowner "should have become aware of it and effected remedial measures." *Id.* Further, the notice must be specific, and "neither a general awareness" nor knowledge of "some other dangerous condition" is sufficient to charge the landowner with notice of the specific defect at issue. *Id.*

1. Plaintiffs have failed to allege any facts that could plausibly establish any defect in Defendants' security measures.

Here, Plaintiffs have failed to allege any specific defect with Defendants' systems in the first place, let alone allege that Defendants had any advance notice of any such defect. Instead, Plaintiffs provide only conclusory allegations. Regarding a purported defect, Plaintiffs allege

only conclusory allegations that Defendants had "unsecure and inadequate data security practices and procedures" (Compl. ¶ 4); "did not employ the required appropriate security to detect intrusions" (Compl. ¶ 25); failed to "protect" or "safeguard" Plaintiffs' PII/PHI (Compl. ¶¶ 112-113); and "failed to monitor its computer systems and/or implement and maintain security controls" (Compl. ¶¶ 114-115).[6] The Plaintiffs' pleading obligation "requires more than labels and conclusions" and "a plausible entitlement to relief exists when the allegations in the complaint move the plaintiff's claims across the line separating the conclusory from the factual, and the factually neutral from the factually suggestive." *Zembiec*, 766 F.Supp.2d at 492, *quoting Bell Atl. Corp.,* 550 U.S. at 555. These conclusory allegations fail to identify any *facts* that could plausibly establish that any defect in Defendants' security practices existed and that this defect contributed to cause the subject ransomware attack.

Rather than allege facts, Plaintiffs' complaint essentially takes the position that Defendants are automatically liable for any third-party criminal acts by mere virtue of the fact that the criminal ransomware attack occurred. Essentially, Plaintiffs ask the Court to hold businesses like Defendants strictly liable for the criminal acts of others. However, there is no basis in New York law for the imposition of such ***strict liability*** for third-party criminal acts. *See Estate of Faughey v. New IG Assoc.*, L.P., 52 N.Y.S.3d 12 (1st Dept. 2017) (where office landlord provided security measures including "24/7 doorman coverage, surveillance cameras, controlled building access, and functioning locks on the doors," landlord was not liable for criminal attack on premises because it was "purely speculative that additional security measures" could have deterred the "premeditated" attack).

---

[6] Plaintiffs' complaint has a section entitled "Defendant Failed to Heed FTC Warnings or Comply with FTC Guidelines," but the actual allegations in that section merely discuss the FTC's guidelines in general, and do not actually allege that Defendant failed to comply with any particular provision of the guidelines. (Compl. ¶ 55-60).

Further, Plaintiffs' conclusory allegations in this case are distinguishable from other data breach cases where the court found sufficient allegations of negligence based on specific factual allegations of defective security measures. *See e.g., Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739 (S.D.N.Y. 2017) (where defendant's employee fell for a phishing attack, plaintiffs alleged that defendant's practices were defective based on defendant's failure to train employees on cybersecurity measures such as recognizing phishing attacks and responding appropriately); *Wallace v. Health Quest Systems, Inc.*, 2021 WL 1109727 (S.D.N.Y., Mar. 23, 2021) (where defendant fell for a phishing attack, plaintiffs alleged that defendant's practices were defective based on failure to implement "multi-factor authentication, appropriate training, and data encryption"); *In re Equifax, Inc.*, 362 F.Supp.3d 1295 (defendant was the subject of several prior data breaches, outside cybersecurity experts had reported on flaws in defendant's security, and before the breach the Department of Homeland Security issued a warning about the precise vulnerability at issue and recommending implementation of a patch, but defendant never implemented the patch). No such allegations exist in Plaintiffs' complaint. Accordingly, this Court should dismiss Plaintiffs' negligence claim for failure to allege facts that could plausibly establish a defect in Defendants' security measures.

2. Plaintiffs have failed to allege any facts that could plausibly establish notice of any defect.

As detailed above notice of a security or safety defect must be specific. Plaintiffs do not allege any facts that could plausibly establish any specific defect in Defendants' security measures, let alone any facts that could plausibly establish that Defendants had notice of any such defect. Rather, Plaintiffs make generalized allegations about ransomware incidents in the aggregate, but such allegations could not possibly establish that Defendants had either actual or constructive notice of a specific defect in their systems that contributed to cause the subject ransomware attack.

Again, Plaintiffs' conclusory allegations in this case are distinguishable from other data breach cases where courts found that plaintiffs stated a claim for negligence based on specific factual allegations of prior notice. *See e.g. Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739 (S.D.N.Y. 2017) (defendant whose e-mail system was hacked by a phishing attack had notice of the vulnerability because its own website warned clients that cyberattacks "are neither new nor infrequent" and cautioned clients never to send sensitive information via e-mail because e-mail "is generally not secure" and is the method of communication that is "most vulnerable to hacking"); *Cohen v. Northeast Radiology, P.C.*, 2021 WL 293123 (S.D.N.Y. Jan. 28, 2021) (defendant had notice of flaws in its system when a group of cybersecurity researches notified defendant of the flaws, and defendant failed to take any action until a newspaper published a story about the researchers' findings); *In re Equifax, Inc.*, 362 F.Supp.3d 1295 (defendant had notice because it was the subject of several prior data breaches, outside cybersecurity experts had reported on flaws in defendant's security, and before the breach the defendant disseminated internally a warning from the Department of Homeland Security about the precise vulnerability at issue and recommending implementation of a patch, but never implemented the patch). Accordingly, this Court should dismiss Plaintiffs' negligence claim for failure to allege facts that could plausibly establish that Defendants had notice of a security defect in its network.

E. This Court should also dismiss Plaintiff's negligence claim for failure to allege any facts that could plausibly establish that the subject ransomware attack was reasonably foreseeable.

Again, Defendants deny that they have any relationship with the Plaintiffs that could create a duty to protect the Plaintiffs from the criminal conduct of third parties. However, even if Defendants had such a duty, the criminal harm must still be shown to be foreseeable for a negligence claim to be plausible. *See, e.g. Mason v U.E.S.S. Leasing Corp.*, 96 N.Y.2d 875, 878 (N.Y. Ct. App. 2001) (explaining that whether prior criminal activity makes future criminal act

reasonably foreseeable "depend[s] on the location, nature and extent of those previous criminal activities and their similarity, proximity or other relationship to the crime in question"). "To establish that criminal acts were foreseeable, the criminal conduct at issue must be shown to be reasonably predictable based on the prior occurrence of the same or similar criminal activity at a location sufficiently proximate to the subject location." *Karim v. 89th Jamaica Realty Co.*, 7 N.Y.S.3d 488 (2nd Dept. 2015).

Here, Plaintiffs allege only that healthcare providers in general are subjects of ransomware attacks. (Compl. ¶¶ 47-54). However, these generalized allegations are insufficient to plausibly establish that a criminal ransomware attack on Defendants' system was reasonably foreseeable. For example, Plaintiffs fail to allege any facts regarding the specific security system utilized by the Defendants, or that a specific security system has been previously targeted by ransomware actors. Accordingly, this Court should dismiss Plaintiffs' negligence claim because Plaintiffs have failed to allege any facts that could plausibly establish that the subject ransomware attack on Defendant's specific network was reasonably foreseeable.

IV. This Court should dismiss Plaintiffs' claims for failure to allege cognizable damages.

Damages are a necessary element of the Plaintiffs' negligence and breach of contract claims. However, as detailed below, Plaintiffs fail to allege any cognizable damages. Accordingly, this Court should dismiss Plaintiffs' negligence and breach of contract claims.

A. Under New York law, the mere risk of future harm is insufficient to impose present liability against a defendant.

New York law is well established that a "threat of harm is insufficient to impose liability against a defendant in a tort context." *Caronia v. Philip Morris USA, Inc.*, 22 N.Y.3d 439, 446 (2013); *See Also Strohm v. New York, L.E. & W.R. Co.*, 96 N.Y. 305, 306 (NY Ct. App. 1884) ("To entitle a plaintiff to recover present damages, for apprehended future consequences, there must be such a degree of probability of their occurring, as amounts to a reasonable certainty that

they will result from the original injury"). Modern precedents require an expense to be "reasonably certain to be incurred" to be recoverable. *Schultz v. Harrison Radiator Div. General Motors Corp.*, 90 N.Y.2d 311, 321 (NY Ct. App. 1997).

Following these well-established principles, multiple courts have found that the mere risk of identity theft in the future is not sufficient damages to support negligence or breach of contract claims arising out of data breaches. *See Wallace,* 2021 WL 1109727, at *8 (S.D.N.Y., 2021) ("Plaintiffs do not plausibly allege they are reasonably certain to incur expenses as a result of their greater exposure to fraud and identity theft" when plaintiff's allegations "raise only the speculative possibility that plaintiffs might, at some point in the future, be victims of fraud and thereby incur monetary or other damages); *Hammond*, 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) (dismissing negligence and breach of contract claims against bank in data breach case, explaining that "increased risk of identity theft is insufficient to support Plaintiffs' substantive claims"); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F.Supp.2d 273 (S.D.N.Y. 2008) (dismissing negligence claims based on theft of laptop containing personal data, when plaintiff failed to establish that identity theft was reasonably certain to occur); *see also Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (affirming dismissal of negligence and breach of contract claims on the merits for lack of damages, explaining that "without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy").

Applying these well-established principles to the subject case, Plaintiffs' negligence and breach of contract claims must be dismissed because the mere risk of future harm, which Plaintiffs concede is neither likely nor imminent, is not a cognizable damage.

B. Plaintiffs cannot manufacture injury by incurring the time and expense of mitigation measures based on the speculative and subjective risk of future harm that Plaintiffs concede is neither likely nor imminent.

"Where plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." *McMorris*, 995 F.3d at 303 (collecting cases). "This notion stems from the Supreme Court's guidance in *Clapper*, where it noted that plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'" *Id.* Consistent with these principles, multiple courts have found that time and expenses incurred in protecting against a speculative or subjective fear of future identity theft. *See Khan*, 188 F.Supp.3d at 533 ("incurring costs as a reaction to a risk of harm does not establish standing if the harm sought to be avoided is not itself certainly impending"); *Shafran v. Harley-Davidson, Inc.*, 2008 WL 763177, at *3 (S.D.N.Y., Mar. 20, 2008) (dismissing negligence and breach of contract claims for lack of damages, explaining that "courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy"). Accordingly, Plaintiffs' negligence and breach of contract claims must be dismissed because their voluntary mitigation measures based on Plaintiffs' subjective fear of risks that they concede are neither likely nor imminent are not cognizable damages.

C. Plaintiffs have failed to plausibly allege any diminution in the value of their personal data.

Courts have found that allegations that a data breach has diminished the value of personal information are not actionable unless "the plaintiff also alleges the existence of a market for that information and how the value of such information could have decreased due to its disclosure. *Wallace*, 2021 WL 1109727, *8 (S.D.N.Y., Mar. 23, 2021) (explaining that allegations about the existence of a black-market for private information generally are not sufficient to plausible allege

damages based on diminution in value); *Pena v. British Airways, PLC (UK)*, 2020 WL 3989055, at *3 (E.D.N.Y., 2020) (finding no injury based on alleged diminution in value when plaintiff "has not alleged that he was offered or forewent any opportunity to profit from the sale of his personal information, or that Defendant's data breach in any way diminished the value of his personal information"); *Fero*, 236 F.Supp.3d at 755 (W.D.N.Y., 2017) (mere allegation that data "commands a high price on the black market" is not sufficient to establish an injury); *Khan*, 188 F.Supp.3d at 533 (D. Md., 2016) (finding no injury when plaintiff failed to "explain how the hackers' possession of that information has diminished its value, nor [did] she assert that she would ever actually sell her own personal information").

Here, Plaintiffs have made only generalized allegations about the existence of a black market for PII/PHI, but Plaintiffs have not alleged that any of their data has been sold or offered for sale on any such market, nor have Plaintiffs alleged that they had any intention of selling their own data on such a market or that the subject data breach prohibited them from selling their own data. Plaintiffs' negligence and breach of contract claims must be dismissed because the Plaintiffs have failed to plausibly allege any diminution in the value of their personal data.

D. Plaintiffs have failed to plausibly allege any benefit-of-the-bargain damages when Plaintiffs have not paid anything for Defendants' services.

Plaintiffs cannot plausibly recover damages on a benefit-of-the-bargain basis when they did not pay anything for the practice management services that Defendants provided to healthcare providers. Multiple courts have found that data breach plaintiffs cannot recover for any alleged benefit of the bargain when they did not pay anything specifically for the alleged data security. *See e.g., Gardiner v. Walmart Inc.,* 2021 WL 2520103, at *6 (N.D. Cal., Mar. 5, 2021) ("Plaintiff's allegations do not establish that the cost of the goods he purchased at Walmart included some amount attributable to data security as required to support his benefit of the bargain theory"); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal.

2020) (finding benefit of bargain not a viable theory of damages where plaintiffs did not allege to have paid anything for the services); *Huynh v. Quora, Inc.*, 2019 WL 11502875, at *10 (N.D. Cal., 2019) (same); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (same); *Accord Palka*, 83 N.Y.2d at 587 ("injured noncontracting parties must show that the performance of contractual obligation between others has induced detrimental reliance by them on continued performance and inaction would result not merely in withholding a benefit, but positively or actively in working an injury"). Accordingly, Plaintiffs' negligence and breach of contract claims must be dismissed because the Plaintiffs have failed to plausibly allege any benefit-of-the-bargain damages.

CONCLUSION

For the foregoing reasons, defendants respectfully request that the Court dismiss the Complaint in its entirety with prejudice.

Dated: Buffalo, NY
November 22, 2021

Respectfully submitted,
BECKAGE PLLC

/s/ *Myriah V. Jaworski*
Myriah Valentina Jaworski
Chirag Patel (*pro hac vice*)
Liberty Building
420 Main Street, Suite 1110
Buffalo, NY 14202
716-898-2102
mjaworski@beckage.com
cpatel@beckage.com